2026 年 7 月 7 日

株式会社 NTT データ
NTT ドコモビジネス株式会社

フロンティア AI を活用したサイバーリスク対応サービスを提供開始

～複数のフロンティア AI の検証知見と 10,000 システム以上の運用実績を活用し、脆弱性対応を一貫支援～

株式会社 NTT データ（以下、NTT データ）と NTT ドコモビジネス株式会社（旧 NTT コミュニケーションズ株式会社、以下、NTT ドコモビジネス）は、フロンティア AI を活用したサイバーリスク対応サービス（以下、本サービス）を 2026 年 7 月 31 日より提供開始します。本サービスは、脅威・脆弱性の発見から影響評価、優先度判断、修復方針の策定、修復対応、継続運用までを一貫して支援します。

NTT データと NTT ドコモビジネスは国内外のフロンティア AI 提供パートナーとの密な連携を通じて、複数のフロンティア AI 技術の評価・検証を実施し、脅威・脆弱性の発見や分析に加え、影響評価、優先度判断、修復方針策定における有効性を確認しました。また、両社のシステム開発・脆弱性診断の経験を活かし、重要システムに求められる運用要件やセキュリティ要件を踏まえた適用可能性を確認・評価しました。

これらの検証結果を踏まえ、本サービスでは、フロンティア AI による分析能力、NTTDATA-CERT をはじめとする両社のサイバーセキュリティ専門組織の知見や、10,000 システム以上のミッションクリティカルシステムで培った管理・運用知見、そして NTT ドコモビジネスが重要インフラ事業者として培ってきたサービス運用とセキュリティ対策のノウハウを組み合わせ、業務影響や運用制約を踏まえた対応方針を提示します。これにより、お客さまは限られた人員でも優先度の高い対策を効率的に実施できます。

【背景】

フロンティア AI の進展により、脅威・脆弱性の発見・分析能力は飛躍的に向上しています。一方で、企業・組織においては、大量に検知される脆弱性や脅威情報の中から、自社システムへの影響、資産の重要度、悪用可能性、業務影響、運用制約を踏まえ、何を優先的に対処すべきかを判断し、修復までつなげることが最も重要な課題となっています。加えて、セキュリティ人材の不足や、脆弱性対応・監視・インシデント対応に係る運用負荷の増大により、限られた体制で優先度の高い対策を迅速かつ継続的に実行することが求められています。また、政府も政府全体のサイバーセキュリティ対策パッケージ「Project YATA-Shield」において、高性能 AI 時代を見据えた重要インフラ事業者などのサイバーセキュリティ対策強化を推進しています。

国内外のフロンティア AI 提供パートナーと密に連携し、複数のフロンティア AI 技術を評価・検証した結果、脅威・脆弱性の発見・分析に加え、影響評価や優先度判断、修復方針策定への有効性を確認しました。その結果を踏まえ、両社は本サービスを提供します。

【概要（特長）】

本サービスは、フロンティア AI による高度な分析と NTT グループが擁する国内トップレベルのセキュリティ専門組織の知見を組み合わせ、脅威・脆弱性の発見から影響評価、優先度判断、修復方針策定、修復対応、継続運用までを一貫して支援します。

フロンティア AI が脅威・脆弱性情報を分析して提示した対応候補に対し、サイバーセキュリティ専門組織が検証することで、お客さまのシステム構成や業務影響を踏まえた対応方針を策定します。これにより、限られた人員でも優先度の高い対策を効率的に実施できます。

さらに、NTT データ、NTT ドコモビジネスを中心としたネットワーク、クラウド、AI 基盤、セキュリティ監視、システム運用の知見を結集し、お客さまの環境に応じた最適な運用体制を提供します。

■本サービスの主な特長

1. 脅威・脆弱性の発見から修復・継続運用までを一貫支援

脅威・脆弱性の発見から影響評価、優先度判断、修復方針の策定、修復対応、継続運用までを一貫して支援します。AI による分析とセキュリティ専門家の知見を組み合わせることで、業務影響や運用制約を踏まえた実効性の高いセキュリティ対策を実現します。これにより、お客さまは脆弱性対応の各工程を分断せず、継続的な運用改善につなげられます。

2. 複数のフロンティア AI を検証した知見を活用

NTT データが国内外のフロンティア AI 提供パートナーとの連携を通じて、複数のフロンティア AI 技術を評価・検証しました。本評価・検証では、脅威・脆弱性の発見や分析、影響評価、優先度判断、修復方針策定における有効性を確認しています。本サービスでは、これらの検証で得た知見を活用し、特定の AI 技術に依存しない分析・判断支援を提供します。また、お客さまのセキュリティ要件、運用要件、利用環境を踏まえ、用途に応じた AI 技術や運用方式の選択肢を提示します。

3. サイバーセキュリティ専門組織の知見を組み合わせ、優先度の高い対策を提示

フロンティア AI が分析した結果を、NTTDATA-CERT をはじめとする両社のサイバーセキュリティ専門組織が検証し、資産重要度、悪用可能性、業務影響、運用制約を踏まえて対応の優先度を判断します。これにより、お客さまは限られた人員でも、優先度の高い対策を効率的に実施できます。

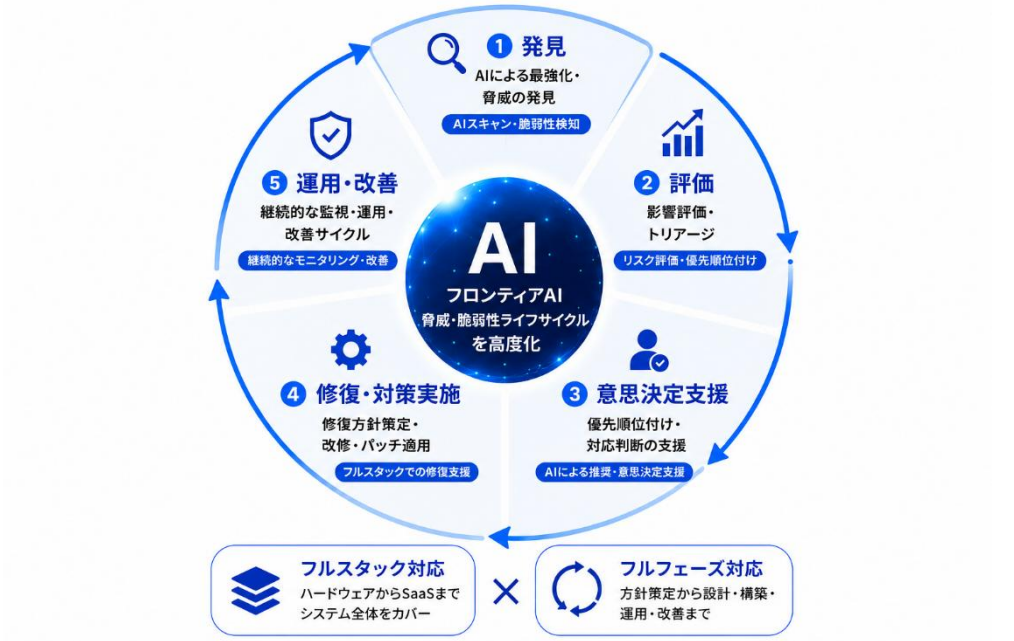
4. フルスタック・フルフェーズによる包括的な支援

ハードウェア、ネットワーク、クラウド、OS、ミドルウェア、OSS・ライブラリ、アプリケーション、SaaS までのシステム全体を対象としたフルスタック対応を提供します。また、コンサルティングから設計・構築、修復、監視、継続的な運用・改善まで、フルフェーズで支援します。これにより、システム全体のリスクを横断的に把握し、設計・運用の両面から対策を進められます。

5. NTT グループの総合力による AI 時代のセキュリティ運用

NTT データと NTT ドコモビジネスを中心に、ネットワーク（NaaS）、クラウド、AI 基盤、セキュリティ監視（AI SOC）、システム運用の知見を結集し、お客さまに最適なセキュリティ運用を提供します。

また、両社の金融・公共・製造・流通・重要インフラなど 10,000 以上のミッションクリティカルシステムの管理・運用で培った知見と、NTT ドコモビジネス自ら重要インフラ事業者として提供するサービスとセキュリティ対策のノウハウを活用し、パッチ適用が困難な環境でも、設定変更、アクセス制御、監視強化などを組み合わせた修復方針を策定します。これにより、お客さまは業務継続性に配慮した対策を選択できます。



図：本サービスの支援範囲

【今後について】

両社は今後、国内外の AI パートナーとの連携をさらに強化し、フロンティア AI の進化に即した継続的な対応やお客さまの要件に応じたソブリン AI 環境への対応を進めます。また、AI 時代に求められる Security for AI と AI for Security の取り組みを拡充するとともに、NTT グループ各社の技術・サービスを結集し、安全なデジタル社会の実現に貢献します。

＊文章中の商品名、会社名、団体名は、各社の商標または登録商標です。